

CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Matthew T. Theriault (SBN 244037)
mtheriault@clarksonlawfirm.com
Bahar Sodaify (SBN 289730)
bsodaify@clarksonlawfirm.com
9255 Sunset Blvd., Suite 804
Los Angeles, CA 90069
Tel: (213) 788-4050
Fax: (213) 788-4070

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

LISA OHLWEILER, individually and on behalf of all others similarly situated,

Plaintiff,

VS.

ZOOM VIDEO COMMUNICATIONS,
INC., a Delaware Corporation,

Defendant.

Case No.

CLASS ACTION COMPLAINT

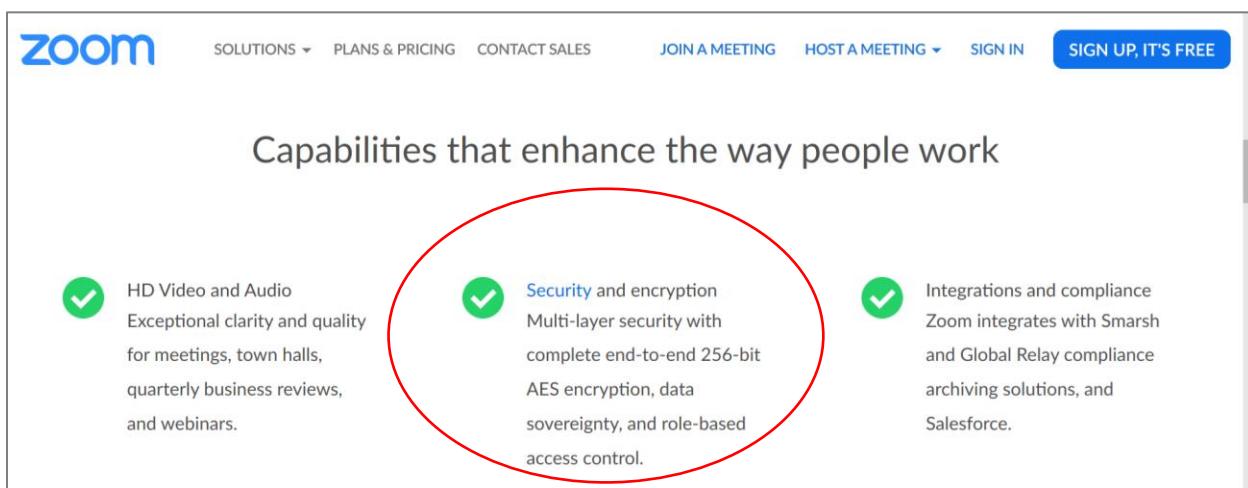
1. VIOLATION OF CALIFORNIA BUSINESS & PROFESSIONS CODE § 17200, *et. seq.*
 2. VIOLATION OF CALIFORNIA CIVIL CODE § 1750, *et. seq.*
 3. VIOLATION OF CALIFORNIA BUSINESS & PROFESSIONS CODE § 17500, *et. seq.*
 4. VIOLATION OF CALIFORNIA CIVIL CODE § 1798.100, *et. seq.*
 5. NEGLIGENCE
 6. VIOLATION OF CALIFORNIA CONSTITUTION ART 1, § 1
 7. BREACH OF EXPRESS WARRANTY
 8. UNJUST ENRICHMENT

DEMAND FOR JURY TRIAL

DEMAND FOR JURY TRIAL

INTRODUCTION

1 1. Zoom sells the private information of its 200 million users without their
 2 knowledge or permission. Zoom also falsely advertises end-to-end encryption. While
 3 many companies are prioritizing people over profits to fight COVID-19, Zoom is
 4 prioritizing profits over people. Zoom is capitalizing off of the global pandemic by
 5 selling user information to Facebook without user consent. Zoom compounds this
 6 felony by falsely advertising that its software is equipped with end-to-end encryption.
 7 Zoom peddles its products knowing that hackers are accessing to user webcams,
 8 exposing its users to extreme invasions of privacy.



19 2. Plaintiff brings this class action on behalf of all similarly situated
 20 consumers who used and/or purchased the Zoom software Product believing that the
 21 Product was secure and that their information was safe.

22 3. Due to the challenges associated with the COVID-19 pandemic, Zoom's
 23 popularity has skyrocketed in recent months. Businesses, schools, and other
 24 consumers are working to find the most efficient way to operate and communicate
 25 while quarantined at home. As a result, many of these organizations are turning to
 26 Zoom's video conferencing software.

27 ///

28 ///

1 4. Zoom consistently violates its duty to implement and maintain
2 reasonable security practices, and misleads consumers about the security benefits of
3 the Product.

4 5. Zoom collects private information about Zoom users and discloses this
5 information to Facebook and other third parties for financial gain. Zoom intentionally
6 omits this fact from its privacy policy and misleads reasonable consumers to believe
7 that the information they share is private.

8 6. Zoom claims to offer users the privacy and protection of end-to-end
9 encryption, the most secure form of internet communication. In reality, Zoom does
10 not offer end-to-end encryption, and its software cannot even support such security
11 measures. Zoom accesses private information that users share on the Zoom network.

12 7. Zoom fails to remedy a known vulnerability that allows hackers and other
13 websites to forcibly join a user to a Zoom call without their permission. This has led
14 to serious invasions of privacy and allows hackers to target users with specific
15 advertisements.

16 8. Plaintiffs seek injunctive relief and restitution against Zoom for false and
17 misleading advertising in violation of Business and Professions Code Section 17200,
18 et seq., Business and Professions Code Section 17500, et seq., and Civil Code Section
19 1750, et seq., and for violating the Consumer Privacy Act. Zoom made and continues
20 to make these false and misleading statements in its advertising of the Product. Zoom
21 also continues to invade the privacy of innocent users and leave them vulnerable to
22 security threats. Compliance with remedial statutes like those underlying this lawsuit
23 will benefit Plaintiffs, the putative class, consumers, and the general public.

24 9. The false and misleading advertising of the Product violates the
25 California Consumers Legal Remedies Act, particularly California Civil Code
26 Sections 1770(a)(5), 1770(a)(7), and 1770(a)(9). As such, Zoom has committed per
27 se violations of Business and Professions Code Section 17200, et seq., and Business
28 and Professions Code Section 17500.

PARTIES

10. Plaintiff Lisa Ohlweiler is an individual residing in Los Angeles, California. Plaintiff purchased and used Zoom in California within the last four (4) years of the filing of this Complaint. Specifically, Plaintiff used the Product while working from home during the current stay-at-home order. Plaintiff relied upon the privacy policy and advertising of the Product, including, Defendant's claims that it would not share private user information with Facebook and that the Product is secure. These privacy policy and advertising statements were prepared and approved by Defendant and its agents and disseminated statewide and nationwide, as well as designed to encourage consumers to purchase the Product. Plaintiff would not have purchased or used the Product, if she had known that the advertising as described herein was false, misleading, and/or deceptive.

11. Zoom Video Communications, Inc. is a Delaware corporation headquartered in San Jose, California. Zoom Video Communications, Inc. maintains its principal place of business at 55 Almaden Blvd. 6th Floor, San Jose, CA 95113. Zoom Video Communications, Inc., directly and through its agents, has substantial contacts with and receives substantial benefits and income from and through the United States and/or State of California. Zoom Video Communications, Inc. is one of the owners, manufacturers, and distributors of the Product, and is one of the companies that created and/or authorized the false, misleading, and deceptive claims on the Product website.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. Section 1332(d)(2)(A) because: (i) there are 100 or more class members, (ii) there is an aggregate amount in controversy exceeding \$5,000,000, exclusive of interest and costs, and (iii) there is minimal diversity because at least one Plaintiff and Defendant are citizens of different states.

1 This Court has supplemental jurisdiction over any state law claims pursuant to 28
2 U.S.C. Section 1367.

3 13. Pursuant to 28 U.S.C. Section 1391, this Court is the proper venue for
4 this action because a substantial part of the events, omissions, and acts giving rise to
5 the claims herein occurred in this District: Plaintiff is a citizen of California who
6 resides in this District; Defendant omitted material information and made the
7 challenged false representations to Plaintiff in this District; and Plaintiff purchased
8 and used the Product within this District. Moreover, Defendant receives substantial
9 compensation from sales and user engagement in this District, and Defendant made
10 numerous material omissions and misrepresentations which had a substantial effect
11 in this District involving its label and packaging representations.

12 14. Defendant is subject to personal jurisdiction in California based upon
13 sufficient minimum contacts which exist between Defendant and California.
14 Defendant is authorized to do and is doing business in California.

FACTUAL ALLEGATIONS

15 15. The global COVID-19 pandemic has drastically reshaped the way in
16 which consumers, businesses, and schools communicate. Rather than lending a hand
17 to people in need, Zoom violates the privacy of its millions of users by misusing and
18 exploiting their personal information, and falsely, deceptively, and misleadingly
19 advertising fictitious security benefits of the program.

Zoom Has Capitalized on COVID-19

21 16. The COVID-19 pandemic has affected the world in unthinkable ways.
22 The virus has infected over one million people worldwide and has been fatal to over
23 50,000. Nearly every state, including California, has a stay-at-home order in place.
24 As a result, millions of people are quarantined at home. Businesses and economies
25 across the globe are struggling to survive the effects of this unprecedented challenge.

26 17. Zoom has targeted consumers, businesses, and schools. Business and
27 schools need to communicate with employees and students, and video conferencing

is the most effective way to communicate remotely. Consumers are also using Zoom to socialize and keep in touch with friends and family. There are 200 million people who now consider Zoom to be synonymous with their everyday schedule.¹

18. Zoom has profited off of users' desire to stay connected professionally and personally during this global pandemic and the accompanying stay-at-home orders. Zoom's stock price has increased from \$62 in October of 2019 to as high as \$159.56 in March of 2020.

Zoom Shares Private User Information with Facebook

19. Every time a user downloads or opens the Zoom iOS app (“App”), Zoom shares the user’s personal and private information with Facebook. Zoom is selling, to Facebook, private information of individuals who do not have a Facebook account.

20. The App reports information on the user's device, what time zone and city the user is in, and the wireless phone carrier connected to their device. Zoom also creates and shares a "unique advertiser identifier" that Facebook uses to target the user with specific advertisements.²

21. Zoom uses a Facebook software development kit (SDK) to implement certain features in the Zoom App. The SDK allows users to login to Zoom through their Facebook account.³

22. Apps that use a Facebook SDK share information with Facebook, and Facebook requires companies that use SDKs to warn users of this fact. Facebook's terms clearly state, “[i]f you use our . . . SDKs, you further represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the

¹ Zoom Blog, *A Message to Our Users*,
<https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/> (last visited April 3, 2020).

² Joseph Cox, *Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account*, MOTHERBOARD, https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account (last visited April 3, 2020).

³ Facebook for developers, *APIs and SDKs*, <https://developers.facebook.com/docs/apis-and-sdks> (last visited April 3, 2020).

1 Customer Data collection, sharing and usage.”⁴ Facebook also warns app developers
 2 that “Facebook[] may collect or receive information from your app and other apps
 3 and use that information to provide measurement services and targeted ads.”⁵

4 23. Zoom never received consent to transfer user data to Facebook. Zoom’s
 5 privacy policy that states Google Ads and Google Analytics “automatically collect
 6 some information about you when you use our Products;” however, Zoom’s privacy
 7 policy fails to mention that it collects and shares any information with Facebook.⁶

8 24. Zoom knows it is violating consumers’ privacy. Zoom released a
 9 statement saying “we were recently made aware that the Facebook SDK was
 10 collecting unnecessary device data.” Zoom further stated that “[u]sers will need to
 11 update to the latest version of our application once it becomes available in order for
 12 these changes to take hold, and we encourage them to do so. We sincerely apologize
 13 for this oversight, and remain firmly committed to the protection of our users’ data.”⁷

14 25. Zoom failed to provide users with accurate disclosures about how it
 15 shares private user information. This violates users’ privacy rights and is completely
 16 at odds with Zoom’s privacy policy.

17 26. Zoom released an updated version of the App that removed the Facebook
 18 SDK. Zoom stated that “[u]sers will need to update to the latest version of our
 19 application . . . in order for these changes to take hold.”⁸

20 27. Many users will not update to the new version of the app. Even if users
 21 do update to the most recent version of the app, their private information has already
 22 been shared with Facebook.

23
 24
 25 ⁴*Id.*

26
 27 ⁵*Id.*

28 ⁶ See Cox, *supra* note 2.

⁷*Id.*

⁸ Zoom Blog, *Zoom’s Use of Facebook’s SDK in iOS Client*,
<https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/>
 (last visited April 3, 2020).

1 28. Zoom receives financial compensation for sharing private user
2 information with Facebook.

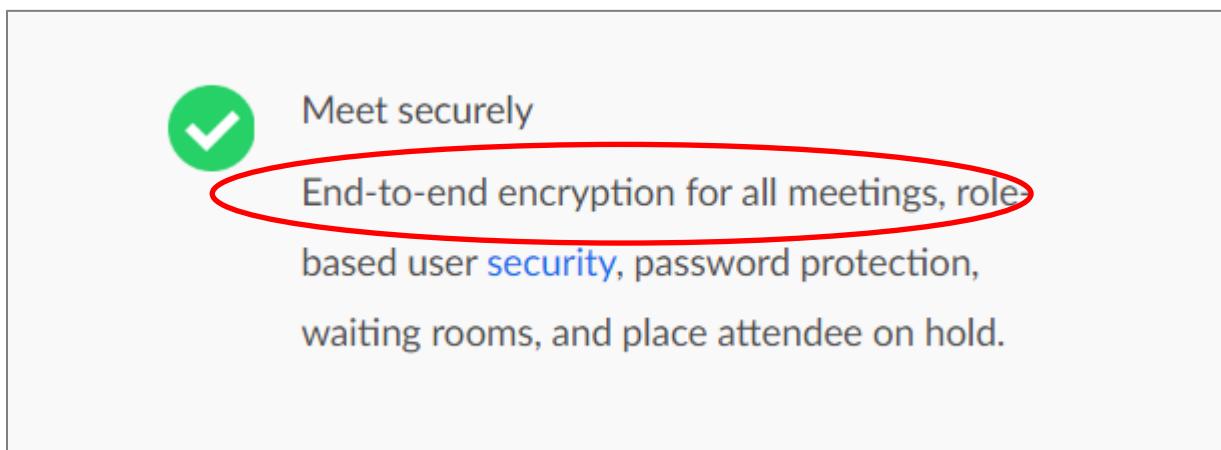
3 29. Consumers are interested in how much of their personal information is
4 being shared with third-party advertisers. Had Plaintiff and the class known that
5 Zoom shared user information with Facebook, they would not have purchased or
6 used Zoom and would have opted to use a different product that did not share their
7 private information with Facebook.

8 **Zoom Falsely Advertises that its Software is Secure**

9 30. Zoom claims that its software offers users the privacy of end-to-end
10 encryption; however, this is false, deceptive, and misleading because Zoom does not
11 use end-to-end encryption.

12 **Figures 1-4** (below): Screenshots taken from Zoom's official website showing
13 that Zoom claims to offer end-to-end encryption.

14 **Figure 1.**



23 ///

24 ///

25 ///

26 ///

27 ///

28 ///

1
2
Figure 2.

3 Protecting your Meetings 4

5 The following in-meeting security capabilities are available to the meeting host:

- 6 ● Secure a meeting with end-to-end encryption
7

8
Figure 3.

9 Protecting your Data 10

11 ● End-to-End Chat Encryption allows for a secured communication where only the intended
12 recipient can read the secured message. Zoom uses both asymmetric and symmetric
13 algorithms to encrypt the chat session. Session keys are generated with a device-unique
14 hardware ID to avoid data being read from other devices. This ensures that the session can not
15 be eavesdropped on or tampered with.
16

17
Figure 4.

18 Enables HIPAA, PIPEDA & PHIPA 19 Compliance 20

21 Zoom's solution and security architecture provides end-to-end encryption and
22 meeting access controls so data in transit cannot be intercepted.
23

24 Zoom does not have access to identifiable health information and we protect and
25 encrypt all audio, video, and screen sharing data.
26

27 Healthcare organizations should contact our sales teams to learn more about our
28 solutions and how they can be configured to comply.
29

1 31. End-to-end encryption is “the most secure” form of privacy for online
 2 communications.⁹ End-to-end encryption security systems prevent anyone
 3 monitoring the network from accessing the information users have communicated,
 4 including the company that owns the network. The only users have who have access
 5 to shared information are the sender and receiver. This keeps user information and
 6 data private and less vulnerable to hacking.

7 32. Rather than providing consumers with end-to-end encryption as
 8 advertised, Zoom uses transport encryption, which is significantly less secure. In fact,
 9 a spokesperson for Zoom stated, “[c]urrently, it is not possible to enable [end-to-end]
 10 encryption for Zoom video meetings.”¹⁰

11 33. Unlike end-to-end encryption, transport encryption allows the company
 12 that owns the network to gain access to user information.¹¹ With transport encryption
 13 in place, Zoom is able to access video and audio content from Zoom meetings that
 14 unsuspecting users believe is secure.

15 34. One computer science expert, Matthew Green, a cryptographer and
 16 computer science professor at Johns Hopkins University, said, “I think they’re doing
 17 this in a slightly dishonest way. It would be nice if they just came clean.”¹²

18 35. Because the software lacks end-to-end encryption, Zoom is able to
 19 monitor video meetings on its software.

20 36. Consumers are indeed interested in the type of security offered by
 21 companies like Zoom and rely on Zoom’s advertising statements to determine which
 22 product to purchase.

23
 24
 25 ⁹ ProtonMail, *End-to-End Encryption*, <https://protonmail.com/blog/what-is-end-to-end-encryption/> (last visited, April 3, 2020).

26 ¹⁰ Micah Lee & Yael Grauer, *Zoom Meetings Aren’t End-to-End Encrypted, Despite Misleading Marketing*, THE INTERCEPT, <https://theintercept.com/2020/03/31/zoom-meeting-encryption/> (last visited, April 3, 2020).

27
 28 ¹¹ *Id.*

¹² *Id.*

1 37. Zoom is aware that reasonable consumers are misled into believing the
 2 Product provides them with end-to-end encryption but has thus far refused to make
 3 any advertising changes to dispel the consumer deception.

4 38. Plaintiff and reasonable consumers reasonably believe Zoom offers users
 5 end-to-end encryption based on its explicit advertising statements.

6 39. Zoom has failed to provide users with accurate disclosures about the type
 7 of security offered with the program. This violates Zoom users' privacy and is at odds
 8 with Zoom's advertisements.

9 **Other Websites Have Access to Users' Webcams**

10 40. Zoom has a vulnerability that allows hackers and other websites to
 11 forcibly join a user to a Zoom video meeting without their permission.

12 41. Zoom has a security patch that is designed to prevent hackers from
 13 gaining access to user webcams. This security patch contains an error that allows
 14 hackers to access user webcams without their knowledge or consent. To gain access,
 15 a hacker simply needs to embed a short coding sequence into their website, and any
 16 Zoom user's video could instantly be compromised.¹³

17 42. This vulnerability affects 13 of Zoom's available applications, including:
 18 Zoom, RingCentral, Telus Meetings, BT Cloud Phone Meetings, Office Suite HD
 19 Meeting, AT&T Video Meetings, BizConf, Huihui, UMeeting, Zhumu, Zoom CN,
 20 EarthLink Meeting Room, Video Conferencia Telmex, & Accession Meeting.

21 43. Zoom's solution to this problem is to provide users the option to have
 22 their video setting turned off when they join a new meeting.¹⁴ However, Zoom cannot
 23 expect users to uniformly adapt to this setting, and millions of webcams are
 24 vulnerable to attack.

25
 26 ¹³ Joseph Cox, *Zoom Vulnerability Lets Hackers Hijack Your Webcam*,
 27 MOTHERBOARD, https://www.vice.com/en_us/article/8xzjj4/zoom-video-conferencing-vulnerability-lets-hackers-turn-on-your-webcam (last visited April 3,
 28 2020).

14 <https://blog.zoom.us/wordpress/2019/07/08/response-to-video-on-concern/>

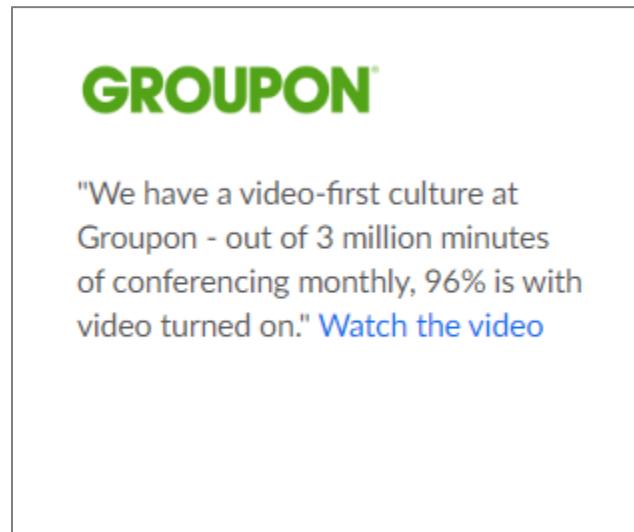
1 44. People use Zoom because it allows them to communicate with video, and
2 several large companies have stated that they use Zoom specifically for its popular
3 video features.

4 45. One of these companies, Groupon, stated, "out of 3 million minutes of
5 conferencing monthly, 96% is with video turned on." True and correct
6 representations of the Groupon's review on Zoom's official website is depicted in
7 Figure 5 below.

8 46. Another company, Sonos, stated that out of all the collaboration tools
9 used by the company, "Zoom video conferencing ranked #1." True and correct
10 representations of the Groupon's review on Zoom's official website is depicted in
11 Figure 6 below.

12 **Figures 5-6** (below): Screenshots taken from Zoom's official website showing
13 that Zoom users prefer Zoom because of its video capabilities.

14 **Figure 5.**



24 ///

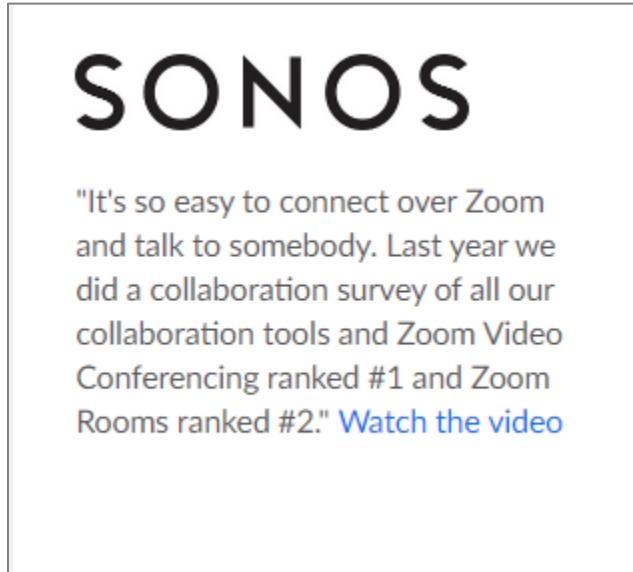
25 ///

26 ///

27 ///

28 ///

Figure 6.



47. Because of the popularity of Zoom's video functionality, users are very unlikely to adopt a setting that turns their cameras off.

48. Plaintiff seeks injunctive relief against Defendant for false and misleading advertising in violation of Business and Professions Code Section 17200, et seq., Business and Professions Code Section 17500, et seq., and Civil Code Section 1750, et seq. Plaintiff also seeks injunctive relief against Defendant for its misuse of private user information in violation of the California Consumer Privacy Act.

49. Defendant made and continues to make these false and misleading statements in its advertising of the Product. Defendant continues to misuse private user information. Compliance with remedial statutes like those underlying this lawsuit will benefit Plaintiff, the putative class, consumers, and the general public. Compliance is the primary litigation objective of this lawsuit.

50. Zoom is marketed, sold, and used throughout California and the United States.

51. Upon information and belief, during the course of its false, misleading, and deceptive advertising campaign, hundreds of millions of people have purchased and used Defendant's Zoom service. Plaintiffs and the Class have suffered injury in

1 fact and have suffered invasion of their privacy rights as a result of Defendant's false
 2 representations and misuse of data and information.

3 **CLASS ALLEGATIONS**

4 52. Plaintiff brings this action on her own behalf and the following class and
 subclass:

- 6 a. **User Class:** "All persons who used the Product in the United States
 7 and/or State of California during the time period of four years prior to the
 8 filing of the complaint through the present."
- 9 b. **Purchaser Subclass:** "All persons who purchased the Product in the
 10 United States and/or State of California for personal use and not for
 11 resale during the time period of four years prior to the filing of the
 12 complaint through the present."

13 53. Excluded from both Classes are Class counsel, Defendants' officers,
 14 directors, and employees, and any individual who received remuneration from
 15 Defendants in connection with that individual's use or endorsement of the Products.

16 54. The Classes are so numerous that their individual joinder herein is
 17 impracticable. On information and belief, the User Class numbers in the tens of
 18 millions or more throughout the United States and/or State of California. On
 19 information and belief, the Purchaser Subclass numbers in the tens of millions or
 20 more throughout the United States and/or State of California. The Classes are
 21 sufficiently numerous because hundreds of thousands of units of the Product have
 22 been sold and tens of millions of people use the Product every day in the United
 23 States and/or California during the time period of four years prior to the filing of the
 24 complaint through the present.

25 55. There is a well-defined community of interest in the questions of law and
 26 fact involved affecting the parties to be represented. The questions of law and fact
 27 common to the Classes predominate over questions which may affect individual
 28

1 Class members. Common questions of law and fact include, but are not limited to,
2 the following:

- 3 a. Whether Defendant's conduct constitutes an unfair method of
4 competition, or unfair or deceptive act or practice, in violation of Civil
5 Code section 1750, et seq.;
- 6 b. Whether Defendant used deceptive representations in connection with
7 the sale of the Product in violation of Civil Code section 1750, et seq.;
- 8 c. Whether Defendant represented the Product has characteristics or
9 quantities that it does not have in violation of Civil Code section 1750,
10 et seq.;
- 11 d. Whether Defendant advertised the Product with intent not to sell it as
12 advertised in violation of Civil Code section 1750, et seq.;
- 13 e. Whether Defendant's advertising of the Product is untrue or misleading
14 in violation of Business and Professions Code section 17500, et seq.;
- 15 f. Whether Defendant knew or by the exercise of reasonable care should
16 have known its advertising was and is untrue or misleading in violation
17 of Business and Professions Code section 17500, et seq.;
- 18 g. Whether Defendant's conduct is an unfair business practice within the
19 meaning of Business and Professions Code section 17200, et seq.;
- 20 h. Whether Defendant's conduct is a fraudulent business practice within the
21 meaning of Business and Professions Code section 17200, et seq.;
- 22 i. Whether Defendant's conduct is an unlawful business practice within the
23 meaning of Business and Professions Code section 17200, et seq.;
- 24 j. Whether Defendant violated its duty to implement and maintain
25 reasonable security procedures and practices in under the California
26 Consumer Privacy Act.

27 56. Plaintiff's claims are typical of the claims of the Classes because their
28 causes of action are based on a substantially similar factual predicate. Plaintiff will

1 fairly and adequately represent and protect the interests of the Classes because she
2 has no conflicts of interest with the Classes. Plaintiff's counsel is adequate counsel
3 because it has vast experience litigating consumer class actions.

4 57. Plaintiff and the Classes have suffered injury in fact and have lost money
5 as a result of Defendant's false representations. Plaintiff and the Classes each
6 purchased and/or used the Product under the false belief that the it had adequate
7 security measures in place and that Defendant would not misuse their personal
8 information. Plaintiff and the Classes would not have purchased and/or used the
9 Product if they had known it does not have adequate security measures in place and
10 that Defendant misuses personal user information.

11 58. A class action is superior to other available methods for fair and efficient
12 adjudication of this controversy. The expense and burden of individual litigation
13 would make it impracticable or impossible for the Classes to prosecute their claims
14 individually.

15 59. The trial and litigation of Plaintiff's Class claims are manageable because
16 Plaintiff and her counsel can litigate the Class claims without the adjudication of
17 numerous individual issues. Individual litigation of the legal and factual issues raised
18 by Defendant's conduct would increase delay and expense to all parties and the court
19 system. Proceeding as a class action in this case presents far fewer management
20 difficulties and provides the benefits of a single, uniform adjudication, economies of
21 scale, and comprehensive supervision by a single court.

22 60. Defendant has acted on grounds generally applicable to both Classes,
23 thereby making final injunctive relief and/or corresponding declaratory relief
24 appropriate with respect to the Classes as a whole. The prosecution of separate
25 actions by individual members of both Classes would create the risk of inconsistent
26 or varying adjudications with respect to individual Class members that would
27 establish incompatible standards of conduct for Defendant.

61. Absent a class action, Defendant will likely retain the benefits of their wrongdoing. Because of the small size of the individual Classes members' claims, few, if any, Class members could afford to seek legal redress for the wrongs complained of herein. Absent a representative action, the Classes will continue to suffer losses and Defendant will be allowed to continue these violations of law and to retain the proceeds of their ill-gotten gains.

COUNT ONE:

Violation of California Unfair Competition Law,
Business & Professions Code Section 17200, et seq.

(By Plaintiff against Defendant)

62. Plaintiff repeats and realleges all allegations of the previous paragraphs, and incorporates the same as if set forth herein at length.

63. This cause of action is brought pursuant to Business and Professions Code Section 17200, et seq., on behalf of both Classes.

A. “Unfair” Prong

64. Under California's False Advertising Law, Cal. Bus. & Prof. Code Section 17200, et seq., a challenged activity is "unfair" when "any injury it causes outweighs any benefits provided to consumers and the injury is one that the consumers themselves could not reasonably avoid." *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

65. Defendant, in its advertising of the Product, makes false and misleading statements regarding the quality and characteristics of the Product, particularly that it offers users end-to-end encryption adequately protects user information with secure privacy measures. Zoom prominently states these characteristics in advertisements and on its official website.

66. Defendant's false and deceptive advertising as alleged herein does not confer any benefit to consumers.

1 67. Defendant's false and deceptive advertising as alleged herein causes
2 injuries to consumers, who do not receive a product consistent with their reasonable
3 expectations.

4 68. Defendant's false and deceptive advertising as alleged herein causes
5 injuries to consumers, who end up purchasing and using a Product that is not as
6 advertised.

7 69. Consumers cannot avoid any of the injuries caused by Defendant's false
8 and deceptive advertising.

9 70. The injuries caused by Defendant's false and deceptive advertising
10 outweighs any benefits.

11 71. Defendant's advertising of the Product, as alleged herein, is false,
12 deceptive, misleading, and unreasonable and constitutes an unfair business practice
13 within the meaning of California Business and Professions Code Section 17200.

14 72. Defendant could have furthered its legitimate business interests in ways
15 other than by advertising the Product unfairly; but they did not, because had they
16 done so, consumers would not have purchased the Product.

17 73. All of the conduct alleged herein occurs and continues to occur in
18 Defendant's business. Defendant's advertising of the Product led and continues to
19 lead reasonable consumers to believe that the Product offers end-to-end encryption
20 and securely protects user information and privacy through a pattern or generalized
21 course of conduct repeated on approximately thousands of occasions daily.

22 74. Pursuant to Business and Professions Code Sections 17203, Plaintiff and
23 the Classes seek an order of this Court enjoining Defendant from continuing to
24 engage, use, or employ their unfair business practices.

25 75. Plaintiff and the Classes have suffered injury-in-fact and have lost money
26 as a result of Defendant's unfair conduct. Specifically, Plaintiff and the Classes
27 purchased or used a Product that was different from what they were reasonably
28 expecting to receive when they decided to use the Product. Plaintiff and the Classes

would not have purchased the Product but for the representations by Defendant that the Product is equipped with end-to-end encryption and adequately protects user information with secure privacy measures.

76. Plaintiff would use the Product in the future if the Product actually provided end-to-end encryption and adequately protected user information with secure privacy measures, or if Defendant's advertising dispelled any confusion about the Product's security features.

B. “Fraudulent” Prong

77. California Business and Professions Code Section 17200, et seq., prohibits fraudulent conduct, defined as conduct that is likely to deceive members of the public. A business practice is “fraudulent” if it actually deceives members of the consuming public.

78. Defendant, in its advertising of the Product, makes false and misleading statements regarding the quality and characteristics of the Product, particularly that it offers users end-to-end encryption and adequately protects user information with secure privacy measures. These advertising claims appear prominently in advertisements for the Product and on Zoom's official website.

79. Defendant's false and deceptive advertising as alleged herein is likely to deceive the members of the public.

80. Defendant's advertising of the Product, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes a fraudulent business practice in violation of California Business & Professions Code Section 17200.

81. Defendant knew that the representations it made and continues to make about the Product are false, misleading, and deceive reasonable consumers.

82. Defendant could have furthered its legitimate business interests in ways other than by advertising the Product fraudulently.

83. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's advertising of the Product led and continues to lead reasonable consumers to believe that the Product offers end-to-end encryption and adequately protects user information with secure privacy measures through a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

84. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the Classes seek an order of this Court enjoining Defendant from continuing to engage, use, or employ their fraudulent business practices.

85. Plaintiff and the Classes have suffered injury-in-fact and have lost money as a result of Defendant's fraudulent conduct. Specifically, Plaintiff and the Classes purchased or used a Product that was different from what they were reasonably expecting to receive when they decided to use the Product. Plaintiff and the Classes would not have purchased the Product but for the representations by Defendant that the Product is equipped with end-to-end encryption and adequately protects user information with secure privacy measures.

86. Plaintiff would use the Product in the future if the Product actually provided end-to-end encryption and adequately protects user information with secure privacy measures, or if Defendant's advertising dispelled any confusion about the Product's security features.

C. “Unlawful” Prong

87. California Business and Professions Code Section 17200, et seq., identifies violations of any state or federal law as “unlawful practices that the unfair competition law makes independently actionable.” *Velazquez v. GMAC Mortg. Corp.*, 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

88. Defendant, in its advertising and packaging of the Product, makes false and misleading statements regarding the quality and characteristics of the Product, particularly that it offers users end-to-end encryption and adequately protects user

1 information with secure privacy measures. These advertising claims appear
2 prominently in advertisements for the Product and on Zoom's official website.

3 89. Defendant's advertising of the Product, as alleged in the preceding
4 paragraphs, violates California Civil Code Section 1750, et. seq., California Business
5 and Professions Code Section 17500, et. seq., California's Sherman Law, and the
6 California Business and Professions Code Section 12606.2, et seq.

7 90. Defendant's advertising of the Product, as alleged in the preceding
8 paragraphs, is false, deceptive, misleading, and unreasonable and constitutes
9 unlawful conduct.

10 91. Defendant knew or should have known of its unlawful conduct.

11 92. As alleged in the preceding paragraphs, the misrepresentations by
12 Defendant alleged herein constitute an unlawful business practice within the meaning
13 of California Business and Professions Code section 17200.

14 93. Defendant could have furthered its legitimate business interests in ways
15 other than by advertising the Product unlawfully.

16 94. All of the conduct alleged herein occurs and continues to occur in
17 Defendant's business. Defendant's advertising of the Product led and continues to
18 lead reasonable consumers to believe that the Product offers end-to-end encryption
19 and adequately protects user information with secure privacy measures through a
20 pattern or generalized course of conduct repeated on approximately thousands of
21 occasions daily.

22 95. Pursuant to Business and Professions Code Sections 17203, Plaintiff and
23 the Classes seek an order of this Court enjoining Defendant from continuing to
24 engage, use, or employ its unlawful business practices.

25 96. Plaintiff and the Classes have suffered injury-in-fact as a result of
26 Defendant's unlawful conduct. Specifically, Plaintiff and the Classes paid for a
27 Product that is different from what they were reasonably expecting to receive when
28 they decided to make their purchases. Plaintiff and the Classes would not have

1 purchased the Product but for the representations by Defendant that it is equipped
2 with end-to-end encryption and adequately protects user information with secure
3 privacy measures.

4 97. Plaintiff would use the Product in the future if the Product actually
5 provided end-to-end encryption and adequately protects user information with secure
6 privacy measures, or if Defendant's advertising dispelled any confusion about the
7 Product's security features.

8 **COUNT TWO**

9 **Violation of California Consumers Legal Remedies Act,**
10 **California Civil Code Section 1750, et seq.**

11 (By Plaintiff against Defendant)

12 98. Plaintiff repeats and realleges all allegations of the previous paragraphs,
13 and incorporates the same as if set forth herein at length.

14 99. Plaintiff brings this cause of action pursuant to Civil Code Section 1750,
15 et seq., the Consumers Legal Remedies Act ("CLRA"), on her own behalf and on
16 behalf of both Classes.

17 100. There are questions of law and fact common to the Classes, which
18 questions are substantially similar and predominate over questions affecting the
19 individual members of the Classes, including but not limited to those questions listed
20 above.

21 101. The practices described herein, specifically Defendant's advertising and
22 sale of the Product, were intended to result in the sale of the Product to the consuming
23 public and violated and continue to violate the CLRA by (1) using deceptive
24 representations in connection with the Product; (2) representing the Product has
25 characteristics and quantities it does not have; and (3) advertising the Product with
26 intent not to sell it advertised.

27 102. Defendant fraudulently deceived Plaintiff and the Classes by
28 misrepresenting the Product as having characteristics and quantities which it does not

1 have, e.g., that the Product is equipped with end-to-end encryption and adequately
2 protects user information with secure privacy measures. In doing so, Defendant
3 intentionally misrepresented and concealed material facts from Plaintiff and the
4 Classes. Said misrepresentations and concealment were done with the intention of
5 deceiving Plaintiff and the Classes and depriving them of their legal rights and
6 money.

7 103. Defendant fraudulently deceived Plaintiff and the Classes by advertising
8 the Product with intent not to sell them as advertised, by misrepresenting that it is
9 equipped with end-to-end encryption and adequately protects user information with
10 secure privacy measures when it does not. In doing so, Defendant intentionally
11 misrepresented and concealed material facts from Plaintiff and the Classes. Said
12 misrepresentations and concealment were done with the intention of deceiving
13 Plaintiff and the Classes and depriving them of their legal rights and money.

14 104. Defendant knew or should have known, through the exercise of
15 reasonable care, that the Product's advertising was misleading.

16 105. Defendant's actions as described herein were done with conscious
17 disregard of Plaintiff's rights, and Defendant was wanton and malicious in its
18 concealment of the same.

19 106. Defendant's Product advertising was a material factor in Plaintiff's and
20 the Class members' decisions to purchase and use the Product. Based on Defendant's
21 Product advertising, Plaintiff and the Classes reasonably believed that they were
22 getting a more secure Product than they actually received. Had they known the truth
23 of the matter, Plaintiff and the Classes would not have purchased the Product.

24 107. Plaintiff and the Classes have suffered injury in fact and have lost money
25 as a result of Defendant's unfair, unlawful, and fraudulent conduct. Specifically,
26 Plaintiff paid for a product with security benefits she never received. Plaintiff would
27 not have purchased the Product had she known it did not offer end-to-end encryption
28 or adequately protects user information with secure privacy measures.

108. Defendant's false and misleading advertising claims should be enjoined due to the false, misleading, and/or deceptive nature of Defendant's advertising. In addition, Defendant should be compelled to provide restitution and damages to consumers who paid for the Product they never received due to Defendant's representation that it was equipped with end-to-end encryption and adequately protects user information with secure privacy measures when it did not.

COUNT THREE

**Violation of California False Advertising Law,
Business & Professions Code Section 17500, et seq.**

(By Plaintiff against Defendant)

109. Plaintiff repeats and realleges the allegations set forth in the preceding paragraphs and incorporates the same as if set forth herein at length.

110. Plaintiff brings this cause of action pursuant to Business and Professions Code section 17500, et seq., each on his own behalf and on both Classes.

111. California's False Advertising Law, California Business and Professions Code section 17500, et seq., makes it "unlawful for any person to make or disseminate or cause to be made or disseminated before the public in this state, in any advertising device or in any other manner or means whatever, including over the Internet, any statement, concerning personal property or services, professional or otherwise, or performance or disposition thereof, which is untrue or misleading and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading."

112. Defendant knowingly disseminated misleading claims that the Product is equipped with end-to-end encryption and adequately protects user information with secure privacy measures as a means to mislead the public for financial gain.

113. Defendant controlled the production and advertising of the Product. It knew or should have known, through the exercise of reasonable care that its

1 representations about the security benefits of the Product was untrue, deceptive and
2 misleading.

3 114. Reasonable consumers base their online purchasing decisions on the net
4 impression of a product's official website. Consumers generally do not conduct their
5 own research to clarify the claims on the product website or for any other reason.
6 Instead, the reasonable consumer chooses a product because the manufacturer's
7 website claims lead them to believe the product is equipped with end-to-end
8 encryption and adequately protects user information with secure privacy measures.

9 115. Defendant's action of prominently displaying false, deceptive, and
10 misleading claims about the purported security benefits of the Product on its official
11 website is likely to deceive the reasonable consumer.

12 116. Defendant's actions were false and misleading such that the reasonable
13 consumer is and was likely to be deceived.

14 117. Plaintiff and the Classes have suffered injury in fact and have lost money
15 as a result of Defendant's false representations. Plaintiff and the Classes purchased
16 the Product in reliance upon the claims by Defendant that the Product is equipped
17 with end-to-end encryption and adequately protects user information with secure
18 privacy measures as represented by Defendant's website descriptions and
19 advertising. Plaintiff would not have purchased the Product if she had known that the
20 claims and advertising as described herein were false and misleading.

21 118. As alleged in the preceding paragraphs, the misrepresentations by
22 Defendant of the material facts alleged herein constitutes an unfair, unlawful, and
23 fraudulent business practice within the meaning of California Business & Professions
24 Code section 17500.

25 119. In addition, Defendant's use of various forms of advertising media to
26 advertise, call attention to, or give publicity to the sale of goods or merchandise
27 which are not as represented in any manner constitutes unfair competition, unfair,
28 deceptive, untrue or misleading advertising, and an unlawful business practice within

1 the meaning of Business & Professions Code sections 17200 and 17531, which
 2 advertisements have deceived and are likely to deceive the consuming public, in
 3 violation of Business & Professions Code section 17500.

4 120. Pursuant to Business & Professions Code sections 17203 and 17535,
 5 Plaintiff and the members of the Classes seek an order of this Court enjoining
 6 Defendant from continuing to engage, use, or employ its practice of advertising the
 7 sale and use of the Product. Likewise, Plaintiff and the members of the Classes seek
 8 an order requiring Defendant to disclose such misrepresentations, and additionally
 9 request an order awarding Plaintiff and the Classes restitution of the money
 10 wrongfully acquired by Defendant by means of responsibility attached to
 11 Defendant's failure to disclose the existence and significance of said
 12 misrepresentations.

13 **COUNT FOUR**

14 **Violation of the California Consumer Privacy Act**

15 **Cal. Civ. Code § 1789.100, et seq.**

16 **(By Plaintiff against Defendant)**

17 121. Plaintiff repeats and realleges the allegations set forth in the preceding
 18 paragraphs and incorporates the same as if set forth herein.

19 122. Defendant has violated California Civil Code Section 1798.100(b) of the
 20 California Consumer Privacy Act (“CCPA”) by collecting and sharing private user
 21 information without providing adequate notice.

22 123. Defendant collects personal user information as defined in Civil Code
 23 Section 1789.140, such as their location.

24 124. Defendant has violated California Civil Code Section 1798.150(a). As a
 25 result of Defendant's inability to implement and maintain reasonable security
 26 procedures and practices, Defendant has given Facebook and other third parties
 27 unauthorized access to private user information as alleged herein.

1 125. Defendant has violated its duty to protect the personal information of
2 Plaintiff and the User Class.

3 126. Defendant's violation of its duty directly and proximately caused
4 Plaintiff and members of the User Class to have their personal information collected
5 and shared with Facebook without authorization. Upon information and belief,
6 Defendant is sharing user information with other unknown parties in the same
7 manner as alleged herein.

8 127. Plaintiff and the User Class were injured through violations of legally
9 protected privacy interests, in the form of unauthorized disclosure of personal user
10 information.

11 128. Defendant knew or should have known that it was violating the CCPA
12 by sharing unauthorized information with Facebook. Defendant also failed to
13 safeguard private user information and maintain reasonable security procedures.

14 129. Defendant is a corporation that is organized and operated for the financial
15 benefit of its owners.

16 130. On behalf of the User Class, Plaintiff seeks an order enjoining Defendant
17 from continuing to violate the CCPA as alleged herein.

18 **COUNT FIVE**

19 **Negligence**

20 **(By Plaintiff against Defendant)**

21 131. Plaintiff repeats and realleges the allegations set forth in the preceding
22 paragraphs and incorporates the same as if set forth herein at length.

23 132. Defendant owed a duty to Plaintiff to exercise reasonable care in
24 implementing and maintaining reliable security systems and practices to ensure the
25 safety of Plaintiff and the User Class members' personal information and not
26 disclosing this information to third parties, like Facebook, without informed consent.

133. Defendant breached its duties by, failing to implement and maintain reasonable security protections for users and by disclosing personal user information to third parties, like Facebook, without the consent of its users.

134. But for Defendant's actions and breaches of its duties, Plaintiff and User Class member information would be secure, and third parties, like Facebook, would not have gained access to personal user information.

135. It was foreseeable that Defendant's conduct as alleged herein would harm Plaintiff and the User Class. Plaintiff knew or should have known that its inability to adequately protect user information, and sharing information with third parties, like Facebook, would cause harm to Plaintiff and the User Class.

136. Defendant's breach as alleged herein directly and proximately resulted in Plaintiff's and the User Class's injuries.

137. Plaintiff's and the User Class's damages were proximate and reasonably foreseeable results of Defendant's breach as alleged herein.

138. As a result of Defendant's breach, Plaintiff and the User Class have been damaged in the amount to be determined at trial.

COUNT SIX

Violation of California Constitution, Art. 1 § 1

(By Plaintiff against Defendant)

139. Plaintiff repeats and realleges the allegations set forth in the preceding paragraphs and incorporates the same as if set forth herein at length.

140. Plaintiff and the User Class have a constitutional right to privacy. Plaintiff and the User Class are entitled to protection from Defendant's unauthorized sharing of their information with third parties, like Facebook.

141. Plaintiff and the User Class reasonably expected the Product to keep their personal information private because the Product's privacy policy fails to disclose that Defendant shares this user information with third parties, like Facebook.

142. Defendant's invasion and violation of Plaintiff and the User Class members' privacy rights was serious and substantial.

143. Defendant unlawfully violated Plaintiff's and User Class members' privacy rights. Defendant failed to implement and maintain adequate safety measures to protect personal user information, and disclosed this information to third parties without the consent of Plaintiff and the User Class in a manner that is highly offensive to a reasonable person.

144. Defendant acted in reckless disregard of Plaintiff's and the User Class's privacy rights. Defendant knew or should have known that its conduct highly invasive and offensive to a reasonable person.

145. Defendant's actions directly and proximately resulted in Plaintiff's and User Class members' personal and private information being disclosed and their reasonable expectation of privacy being frustrated. As a result of the conduct alleged herein, Plaintiff and the User Class have suffered injuries and are entitled to appropriate relief.

COUNT SEVEN

Breach of Express Warranty

(By Plaintiff against Defendant)

146. Plaintiff repeats and realleges the all allegations of the previous paragraphs and incorporates the same as if set forth herein at length.

147. Defendant expressly warranted on its website that the Product is equipped with end-to-end encryption. Defendant's claims constitute an affirmation of fact, promise, and/or description of the goods, the Product, that became part of the basis of the bargain and created an express warranty, that the Product would conform to the stated promise. Plaintiff placed importance on Defendant's claims.

148. All conditions precedent to Defendant's liability under this contract have been performed by Plaintiff and the Purchaser Subclass.

149. Defendant breached the terms of this contract, including the express warranties, with Plaintiff and the Purchaser Subclass by not providing a Product that conformed to the advertisements.

150. Defendant's express warranty that the Product is equipped with end-to-end encryption was breached because the Product is not actually equipped with end-to-end encryption.

151. Defendant therefore breached the terms of its express warranty with Plaintiff and the Purchaser Subclass by not providing a Product that conforms to its specific advertising claims.

152. As a result of Defendant's breach of express warranty, Plaintiff and the Purchaser Subclass have been damaged in the amount to be determined at trial.

COUNT EIGHT

Unjust Enrichment

(By Plaintiff against Defendant)

153. Plaintiff repeats and realleges the allegations set forth above and incorporates the same as if set forth herein at length.

154. By means of Defendant's wrongful conduct alleged herein, Defendant knowingly sold the Product to Plaintiff and members of the Purchaser Subclass in a manner that was unfair, unconscionable, and oppressive.

155. Defendant knowingly received and retained wrongful benefits and funds from Plaintiff and members of the Purchaser Subclass. In so doing, Defendant acted with conscious disregard for the privacy rights of Plaintiff and members of the Purchaser Subclass.

156. As a result of Defendant's wrongful conduct as alleged herein, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and members of the Purchaser Subclass.

157. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein.

158. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, without justification, from selling the Product to Plaintiff and members of the Purchaser Subclass in an unfair, unconscionable, and oppressive manner. Defendant's retention of such funds under such circumstances making it inequitable to do so constitutes unjust enrichment.

159. The financial benefits derived by Defendant rightfully belong to Plaintiff and members of the Purchaser Subclass. Defendant should be compelled to return in a common fund for the benefit of Plaintiff and members of the Purchaser Subclass all wrongful or inequitable proceeds received by Defendant.

160. Plaintiff and members of the Purchaser Subclass have no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for judgment and relief on all causes of action as follows:

- A. An order enjoining Defendant from selling the Product as currently advertised;
 - B. Damages in an amount to be determined at trial, together with pre- and post-judgment interest at the maximum rate allowable by law on any amounts awarded;
 - C. Restitution and/or disgorgement in an amount to be determined at trial;
 - D. Punitive damages;
 - E. Reasonable attorneys' fees;
 - F. Costs of this suit; and
 - G. Such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a jury trial on all triable issues.

DATED: April 3, 2020

CLARKSON LAW FIRM, P.C.

/s/ Ryan J. Clarkson
Ryan J. Clarkson, Esq.
Matthew T. Theriault, Esq.
Bahar Sodaify, Esq.

Attorneys for Plaintiff

CLARKSON LAW FIRM, P.C.
9255 Sunset Blvd., Suite 804
Los Angeles, CA 90069